

IN THE UNITED STATES DISTRICT COURT  
DISTRICT OF MARYLAND

Southern Division

IN THE MATTER OF THE SEARCHES OF:

2442 ST. CLAIR DRIVE, TEMPLE HILLS,  
MARYLAND;

A GOLD 2004 BMW SUV WITH VIRGINIA  
LICENSE PLATE NUMBER VVD4387 AND  
VEHICLE IDENTIFICATION NUMBER  
5UXFA13514LU28537;

A BLACK 2006 MERCEDES SEDAN WITH  
VIRGINIA LICENSE PLATE NUMBER  
VXR5729 AND VEHICLE IDENTIFICATION  
NUMBER WDDDJ75X96A057;

A WHITE 1998 FORD TRUCK WITH  
VIRGINIA LICENSE PLATE NUMBER  
VXR5749 AND VEHICLE IDENTIFICATION  
NUMBER 1FTZF1720WNB46350; AND

THE PERSON AND ELECTRONIC DEVICES  
OF RODRIGUEZ RODNEY LOMAX NORMAN

Case No. 17-2261-CBD

Case No. 17-2262-CBD

Case No. 17-2263-CBD

Case No. 17-2264-CBD

Case No. 17-2265-CBD

**FILED UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF  
APPLICATIONS FOR SEARCH WARRANTS**

I, Charles B. Doughty, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. Since March 2005, I have been employed as a Special Agent with the Federal Bureau of Investigation (hereinafter "FBI"). I am currently assigned to the Washington Field Office, Northern Virginia Resident Agency. During my tenure as a Special Agent with the FBI, I have been involved in many criminal investigations, primarily those pertaining to white collar and

*CBD*

and health care fraud. I have participated in federal investigations which have utilized telephone wire interceptions, telephone toll analysis, undercover operations, search and seizure warrants, surveillance, and interviews. Due to my training and experience, I am familiar with allegations of criminal activity including wire fraud, bank fraud, and similar offenses.

2. During the course of my participation in investigations of white collar crimes, I have testified in trial and grand jury proceedings. I have written reports, analyzed records and documents, and served as a monitoring agent on Title III wiretaps where I was not the affiant. Through my employment with the FBI, I have gained knowledge in the use of various investigative techniques including the utilization of wiretaps, physical surveillance, undercover agents, confidential informants and cooperating witnesses, the controlled purchases of illegal narcotics, electronic surveillance, consensually monitored recordings, investigative interviews, financial investigations, the service of administrative and grand jury subpoenas, and the execution of search and arrest warrants.

3. I have participated in the investigation resulting in the affidavit in support of a criminal complaint and arrest warrant that charged RODRIGUEZ RODNEY LOMAX NORMAN in the Eastern District of Virginia with participating in a conspiracy to commit bank fraud and wire fraud, in violation of 18 U.S.C. § 1349. *See* Case No. 1:17-MJ-388 (E.D. Va.). I hereby incorporate Paragraphs 6 to 94 of that affidavit (the "Criminal Complaint Affidavit"), which is attached, as though fully set forth herein.

4. I make this affidavit in support of five applications for search warrants under Rule 41 of the Federal Rules of Criminal Procedure to search the following: the premises known as 2442 St. Clair Drive, Temple Hills, Maryland ("TARGET PREMISES"); a gold 2004 BMW SUV that bears Virginia license plate number VVD4387 and vehicle identification number

("VIN") 5UXFA13514LU28537 ("TARGET VEHICLE 1"); a black 2006 Mercedes sedan that bears Virginia license plate number VXR5729 and VIN number WDDDJ75X96A057 ("TARGET VEHICLE 2"); a white 1998 Ford truck that bears Virginia license plate number VXR5749 and VIN number 1FTZF1720WNB46350 ("TARGET VEHICLE 3"); and the person of NORMAN as well as the area within his control and any electronic devices.

5. The investigation to date, as described in more detail below, has indicated that NORMAN has his their primary residence at the TARGET PREMISES; NORMAN owns and drives both TARGET VEHICLE 1 and 3; and an individual believed to be NORMAN's girlfriend owns TARGET VEHICLE 2, which NORMAN uses.

6. Each place or person to be searched is described further in the Attachment A appended to the corresponding search warrant application. Likewise, the things to be searched for are described further in the Attachment B appended to the corresponding search warrant application.

7. The facts and information contained in this affidavit are based upon my training and experience, participation in this and other investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other federal agents and individuals involved in this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

8. Based on my training and experience and the facts as set forth in this affidavit (including the incorporated portions of the Criminal Complaint Affidavit), there is probable cause to believe that evidence, fruits, or instrumentalities of all of the below crimes ("TARGET OFFENSES") are in the TARGET PREMISES, TARGET VEHICLES, or on NORMAN's person

or in his control: 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1028 (identity theft), § 1029(a) (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud); § 2342 (trafficking of contraband cigarettes); §§ 1956 and 1957 (conspiracy to commit money laundering) (collectively, “Fraud Scheme offenses”); 21 U.S.C. §§ 841 and 846 (conspiracy to distribute oxycodone); and 7 U.S.C. § 2156 (unlawful animal fighting venture).

### **BACKGROUND ON ANIMAL FIGHTING VENTURES**

9. The federal Animal Welfare Act defines “animal fighting venture” as “any event, in or affecting interstate or foreign commerce, that involves a fight conducted or to be conducted between at least 2 animals for purposes of sport, wagering, or entertainment.” 7 U.S.C. § 2156(g)(1). It is illegal to sponsor or exhibit an animal in an animal fighting venture. 7 U.S.C. § 2156(a)(I). It is also illegal to possess, train, sell, buy, transport, deliver or receive an animal for purposes of having the animal participate in an animal fighting venture. 7 U.S.C. § 2156(b). All of these offenses are felonies punishable by up to five years in prison. 7 U.S.C. § 2156(j); 18 U.S.C. § 49.

10. The Secretary of Agriculture is authorized to enforce the Animal Welfare Act, which provides that “[t]he Secretary or any other person authorized by him shall make such investigations as the Secretary deems necessary to determine whether any person has violated or is violating any provision of this section.” 7 U.S.C. § 2156(f). Section 2156(f) also provides that the Secretary “may obtain the assistance of the Federal Bureau of Investigation . . . in the conduct of such investigations, under cooperative agreements with such agencies.”

11. The Animal Welfare Act states that “[a] warrant to search for and seize any animal which there is probable cause to believe was involved in any violation of this section may be issued by any judge of the United States or of a State court of record or by a United States

magistrate judge within the district wherein the animal sought is located.” 7 U.S.C. § 2156(f). Any animal “involved in any violation of this section shall be liable to be proceeded against and forfeited to the United States” in either a civil or criminal proceeding. *Id.*; 28 U.S.C. § 2461.

12. Law enforcement officers with the U.S. Department of Agriculture, Office of the Inspector General, who are part of this dog-fighting investigation have relayed to me the following:

a. In the United States, dog fighting ventures almost always involve “pit bull”-type dogs, which dog fighters prefer for their compact muscular build, short coat, and the aggression that some display toward other dogs. Generally, a dog fight occurs when two dogs are knowingly released by their handlers in a controlled environment to attack each other and fight. The fight ends when one dog withdraws, when a handler “picks up” their dog and forfeits the match, or when one or both dogs die.

b. Because of their conditioning and training, dogs used in animal fighting ventures are almost always housed separately from other dogs – in pens, cages, or on chains, so that they will not hurt or kill other dogs when the handler is absent. Heavy chains are often used when restraining dogs to develop neck strength in dogs used for fighting purposes.

c. Generally, dog fighters fight dogs with a goal of obtaining “Champion” or “Grand Champion” status for their dogs, which is achieved by winning three or five fights, respectively. They maintain contact with other dog fighters around the country, and can generate substantial income from gambling on dog fights and from the sale and breeding of fighting animals.

d. Generally, dog fighters select the strongest, most capable fighting dogs and selectively breed, sell, and fight only those dogs that display particular traits. Some of these

traits are: (1) “gameness” or aggressiveness and propensity to fight other dogs; (2) a willingness to continue fighting another dog despite traumatic and/or mortal injury; and (3) cardiovascular endurance to continue fighting for long periods of time and through fatigue and injury. Dogs displaying these attributes are often bred with other dogs displaying similar traits to enhance the bloodline of these dogs for fighting purposes. Dog fighters such as the individuals described in this affidavit generally keep such dogs solely for fighting purposes.

e. It is a common practice for those involved in training and exhibiting fighting dogs to possess several dogs at one time. This practice is followed for several reasons. First, dog fighters generally maintain a stock of dogs at different weights and both sexes because in dog fights, dogs are matched against other dogs to within a pound of the same weight against dogs of the same sex. Maintaining a stock of several dogs thus increases the odds of owning a dog whose weight meets the requirements for a match being solicited by an opponent. Second, dog fighters also generally maintain multiple dogs in order to selectively breed, sell, and fight dogs displaying certain traits or to otherwise advance a particular dog fighting bloodline.

f. Further, dog fighters generally must possess an inventory of dogs because dogs often die or are badly injured during fights. Possessing multiple dogs also increases the prospects of owning a dog who will become a Champion or Grand Champion. Dog fighters also routinely test and evaluate their dogs to determine those that exhibit aggressive behavior, including against their own dogs.

g. Generally, dogs that lose fights or fail to show “gameness” are often killed. It is not uncommon for dogs that lose matches to be killed in cruel, torturous, and inhumane ways as punishment.

h. Dog fights typically involve consistent practices leading up to and during the fight. Fighting dog owners or handlers enter into a verbal or written contract with their opponent several weeks before the dog fight, often referred to as a “match,” “fight,” or “show.” The owners or handlers agree upon: (1) the sex and set weight of the dogs at the time of the fight; (2) the geographic area in which the fight will occur (the exact location of which is often a guarded secret until shortly before the fight); (3) a referee; (4) the payment of “forfeit” money that is lost if one participant pulls out of the match or if a participant’s dog does not arrive at the agreed-upon weight; and (5) monetary wagers placed by the respective fighters.

i. It can be challenging for dog fighters to find an opponent with a dog of the same weight and sex who is looking to fight that dog at the same time of year, and for a wager that is mutually agreeable to both parties. For that reason, dog fighters rely heavily on each other and on extensive networks of contacts to find an opponent who has a dog of the same weight and sex and who is looking to fight that dog at the same time of the year. The practice is known as “calling out a weight.” Dog fighters often “call out a weight” to known dog fighters in several states, to increase their odds of finding a match. “Calling out a weight” is done by telephone, text message, e-mail, or other electronic communication. It is an integral practice without which many dog fights would not occur.

j. Once a dog fighter locates an opponent and agrees upon terms, the match is “hooked,” or set up. The dog then typically undergoes a conditioning process dog handlers refer to as a “keep.” A “keep” is typically conducted for six to eight weeks before the scheduled match and involves a training program including: treadmills used to run and exercise the dogs away from public view; weight pulls used to increase the dog’s strength and stamina; the use of devices such as “spring poles” and “flirt poles” to build jaw strength and increase aggression;



and the administration of drugs, vitamins, and other medicine. Some of the drugs used, illegal and legal, include steroids to build muscle mass and aggression. Dogs matched for future fights are expected to achieve their established target weight by the scheduled match, much like in human boxing matches, requiring close attention to a dog's routine. Training can take place at a dog fighter's "yard" or indoors away from public view, often in a basement.

k. Although dogs used for fighting are often housed outside, as the match date approaches, a dog in a keep may be housed indoors or near the owner/handler for several reasons. One reason is to prevent the dog from becoming sick or injured by other dogs before the match, which could cause the dog to forfeit and the owner to pay a forfeit fee. Another reason is that dogs in a keep require constant exercise and monitoring, which is easier when the dog is in close vicinity rather than off-site or outside. Dogs intended for fighting purposes are also often housed inside residences if they are injured, ill, pregnant, weaning, or if a dog fighter does not have another location to keep them or wants to keep them out of view.

l. Some dog fighters are selective about who they will sell fighting dogs to, because the success of that dog in the fighting ring will reflect on the seller whose bloodline is represented by the dog. A dog that produces multiple offspring that go on to be "Champions" (*i.e.*, winning three or more dog fights) is bestowed the "Register of Merit" or "R.O.M." title. This provides incentive to the seller to sell dogs to capable dog fighters, with the intention that the dogs will be fought.

m. It is common for those operating dog fighting ventures to maintain pedigrees, books, records, ledgers, and journals relating to the purchase, transportation, sale, breeding, and training of fighting dogs. These materials occur in both hard and electronic copy. Dog fighters often maintain information regarding dog fighting activities in order to stay current



with the dog fighting community. "Underground" dog fighting publications similar to magazines are routinely published and distributed to readers through periodic subscriptions, which describe and report on recent fight details and past results from around the country using coded language. They also describe various "kennels" or dog breeders who raise dogs for animal fighting purposes. In addition, there are online versions of published magazines that serve the same purpose, as well as websites where dog fighters post pedigrees to demonstrate the fighting lineage of their dogs. Dog fighters also maintain detailed ledgers and journals that specifically depict how certain dogs performed during a particular fight, together with the duration and outcome of fights.

n. Dog fighters today tend to communicate via email, text messages, or website chat rooms dedicated to "game dogs." Dog fighters routinely hook matches and exchange documents, tips, photographs, or videos relating to dog fighting activities via electronic means. Dog fighters exchange videos, for example, to demonstrate the strength and gameness of their dogs.

### **PROBABLE CAUSE**

#### **A. Fraud Scheme offenses**

13. An overview of the investigation of NORMAN for the Fraud Scheme offenses is set forth in the incorporated Criminal Complaint Affidavit.

#### **B. Conspiracy to distribute oxycodone or other prescription pain medication**

14. Investigation has also shown that NORMAN and others, including WILLIAMS, may be in a conspiracy to fraudulently obtain and then distribute oxycodone, a Schedule II drug. Investigation has indicated that WILLIAMS has repeatedly obtained prescriptions for oxycodone from a doctor's office in Florida. WILLIAMS is not believed to have a residence or other

significant ties to Florida. According to records checks from Virginia's Prescription Monitoring Program (PMP),<sup>1</sup> WILLIAMS has a prescription for oxycodone written by a doctor in West Palm Beach, Florida. PMP records show that for every month between July 2015 and May 2017, WILLIAMS filled a prescription for 120 tablets of 30 mg oxycodone HCl.

15. In an intercepted wire communication on WILLIAMS's cellphone (authorized by court order, as described in the Criminal Complaint Affidavit) on August 15, 2017, WILLIAMS and an unidentified individual discussed filling prescriptions at particular locations and profiting from sales. In that conversation, WILLIAMS stated, "I'm coming down there. . . . I was just like it fuck it cause I gotta get my fucking scripts filled." In this context "scripts" is believed to mean prescriptions. When asked, "what," WILLIAMS repeated, "I gotta get that, my scripts filled." The unidentified individual on the call asked, "Where you get that? West Virginia still?," to which WILLIAMS responded, "Nah nah, over here. In Arlington."

16. Later in the same conversation, the unidentified individual asked, "Roddoe [NORMAN's nickname] go to the person you go to?" WILLIAMS responded, "Nah Roddoe found his own spot. I don't know where he be going." The following conversation then immediately followed:

UNIDENTIFIED MALE: So he lit then

WILLIAMS: Who Roddoe?

UNIDENTIFIED MALE: Yeah, but he still... [Talking over each other]

WILLIAMS: Yeah but Roddoe.... Huh

---

<sup>1</sup> A description of Virginia's PMP is available at [www.dhp.virginia.gov/dhp\\_programs/pmp/pmp\\_desc.asp](http://www.dhp.virginia.gov/dhp_programs/pmp/pmp_desc.asp). Under that program, pharmacies and physicians are required to report all dispensing of any Schedule II controlled substances, among other things, to the PMP.

UNIDENTIFIED MALE: But he still sell his shit to you though don't he?

WILLIAMS: Nah, I mean, yeah I make my little bread [slang for cash] off of that, yeah

UNIDENTIFIED MALE: Yeah I know, but I'm just saying

WILLIAMS: Yeah

UNIDENTIFIED MALE: Oh of course

WILLIAMS: Yeah, that's 3. Thats 3 in the bag every month. Easy.

UNIDENTIFIED MALE: 3 what? Oh 3 hundred?

WILLIAMS: 3 THOU

UNIDENTIFIED MALE: From him?

WILLIAMS: unnn hn.

Based on my knowledge of this investigation and the context of this conversation, as well as my training and experience, I believe WILLIAMS to state in this August 2017 call that NORMAN is obtaining prescription medication from a pharmacist at "his own spot," which NORMAN is then partially selling to WILLIAMS.

17. The day after this conversation, on August 16, 2017, FBI physical surveillance observed WILLIAMS visit an identified pharmacy in Arlington, Virginia, corroborating WILLIAMS's assertion that he was going to have "scripts" filled in "Arlington."

18. Investigation has shown that both NORMAN and WILLIAMS may have been involved in a conspiracy to distribute oxycodone or other prescription pain medication going back to 2015. Found at WILLIAMS's residence during an August 27, 2015 search (described in the Criminal Complaint Affidavit) were over \$36,000 in cash and a large quantity of pills, which were found in WILLIAMS's bedroom. During this search, officers found multiple prescription-

labeled containers listing WILLIAMS's name, whose labels indicated they contained oxycodone and other prescription drugs.

19. Similarly, text messages uncovered from WILLIAMS's electronic devices that were seized during the August 2015 search of WILLIAMS's residence (described in the Criminal Complaint Affidavit) showed that earlier in 2015, NORMAN appeared to exchange text messages with WILLIAMS regarding obtaining prescriptions and having them filled. For example:

a. On January 28, 2015, NORMAN texted WILLIAMS, "Yeah I'm at the clinic and they got new receptionist that's going ham I was goin have to pee in the cup so I was goin have you link me with someone up here that might have one so it could be in my system." In my training and experience, some doctors require patients receiving pain medication to provide urine samples to prove they are taking the medication as prescribed. My knowledge of this investigation and my training and experience lead me to believe that NORMAN's text message to WILLIAMS suggests that NORMAN is not taking the medication he has been prescribed, and instead is redistributing it.

b. On March 4, 2015, WILLIAMS and NORMAN exchanged the following text messages about "joints," which based on my knowledge, training, and experience I believe in the context of this conversation to refer to prescriptions:

WILLIAMS: Lol oh ight u getting those my joints right out there  
or nah

NORMAN: Yeah I got too many papers. Miami will make 4  
unfilled

WILLIAMS: Yea u stacked up

NORMAN: Walmart has one, this one that I'm grabbing now, one from MIA last month that I'm dropping off tomorrow and then next week when we go OT

NORMAN: Yeah son and I'm down to may last \$100

WILLIAMS: Word me too bro I'm hurt

NORMAN: I need one of these joints filled asap

NORMAN: We lit. I got 120

NORMAN: Hopefully I'll have 240 by tomorrow

I believe that NORMAN's text messages reflect that he obtained 120 pills, and would have 240 by the following day.

20. Based on my training and experience and knowledge of the investigation, I know that prescription pills and paper prescriptions are easily and often concealed in residences, vehicles, and on individuals' persons. For example, in previous investigations I have found prescription papers and/or pills secreted in drawers, briefcases, wallets, prescription bottles, plastic bags, and pockets, among other places. I also know that prescription papers and pills are easily transported, including in cars. For example, in previous investigations I have found prescription papers and/or pills secreted in automobiles, including center consoles, ashtrays, and under floor mats, among other places.

**C. Conspiracy to participate in dog-fighting venture**

21. Your Affiant also believes that NORMAN is engaged in an ongoing conspiracy to sponsor or exhibit an animal in an animal fighting venture from the TARGET PREMISES, where he has been observed during FBI surveillance entering and leaving with dogs, as well as from another location four miles from the TARGET PREMISES in Washington, D.C. that NORMAN also uses. Furthermore, your Affiant believes NORMAN also possesses, trains, and/or transports

animals for participation in animal fighting ventures.

22. This belief stems in part from NORMAN's own statements obtained from court-authorized interceptions of NORMAN's cellphone for wire communications. As described in the Criminal Complaint Affidavit, on July 24, 2017, the Honorable Anthony J. Trenga, U.S. District Judge, Eastern District of Virginia, issued an order authorizing the interception of wire communications occurring to and from AT&T cellular telephone number (202) 600-0192, bearing international mobile equipment identification number (IMEI) 359177077888918, used by NORMAN ("NORMAN's cellphone"). Law enforcement agents listening to the wiretap determined that NORMAN was significantly involved in dog fighting. The supervising wiretap judge was notified of the evidence of this additional crime and on July 26, 2017, Judge Trenga issued an order allowing the U.S. Department of Justice and assisting federal agencies to use the wiretap to intercept wire communications to and from NORMAN's cellphone relating to potential violations of 7 U.S.C. § 2156, the federal Animal Welfare Act.

23. During the period of the wiretap – July 25, 2017 through the present – the intercepted communications on NORMAN's cellphone included conversations between NORMAN and other individuals discussing their involvement in dog fighting ventures, such as possessing and training their fighting dogs and participating in dog fighting matches. Multiple intercepted calls to and from NORMAN's cellphone have appeared to relate to dogfighting. Some examples follow. All conversations described herein occurred on telephone calls lawfully intercepted on NORMAN's cellphone, as described above.

a. In a phone call on August 3, 2017, between NORMAN and an unidentified male, NORMAN stated, "I was like, man, I don't have a dog in my cages that won't fight bro."

b. NORMAN has indicated in phone calls that he keeps dogs at different locations. On a phone call the evening of August 3, 2017, NORMAN stated to a male speaker, "I got to take this trip on down NC man." When asked, "Oh what you got going on?" NORMAN replied, "Nah, you know I keep dogs down there too. I just ain't went down there . . . I got like 7 or 8 down there of age most of them just kids though but they all ready to hook , they finish school just grab them and hook them one at a time." As described above, "hook" is known term related to dog-fighting ventures.

c. NORMAN has described in phone calls breeding various dogs. Later in the same August 2, 2017 conversation described in the preceding paragraph, NORMAN described how he had bred Bruiser to female dogs: "Bruiser was bred to Dragon Lady which is a pure [unintelligible] dog. And all those died. Then he was bred to umm you remember Champion Diablo that double negro male, I bred Bruiser to his sister." On the evening of July 26, 2017, NORMAN spoke on his cellphone with another male about someone who had agreed to help NORMAN with his dogs. When asked, "Oh he know how to work a dog man?" NORMAN responded, "Yeah he worked a dog he worked he worked a champion that we had he worked him for two. He worked a dog that went 3 hrs and 16. He do good with workin a dog. He, I don't know, I second guessed him because, he, I don't know, me and my partner, he do shit totally different. You know what I'm saying? He the way he breed and stuff, he's still chasin that Champion we had, because everybody be asking me and I be asking myself this shit but, it was because of him that we don't run that blood no more." Later on in the conversation, NORMAN described how he "start[ed] winnin with different dogs," "winning with different blood."

d. Relatedly, in the July 26, 2017 conversation described in the preceding paragraph, NORMAN appeared to recount the fate of puppies a female dog had birthed:



NORMAN: the bitch we had had thirteen puppies bro.

[MALE SPEAKER]: Oh

NORMAN: And he, you know let all them mother fuckers die. We got in a bad argument I ran over the house and took what I can get what was left, there was three left and the one I kept, he let his die, out of thirteen, we gave one to my man who we did the breeding with and um, and mine had a hip problem. I ended up putting mine down. My bitch, my bitch would drag her hips across.

e. NORMAN has described on calls an apparent dog fight in which he entered his dog Pryex. Multiple calls on NORMAN's cellphone on July 29, 2017, revealed NORMAN and multiple individuals discussing what appears to be an organized dog fight, with gambling. Beginning at around 5:28 a.m., NORMAN had a phone conversation with a male speaker where they discussed "Shine," "Pablo" and "Pyrex," who based on the context of the conversations are believed to be dogs. NORMAN also discussed meeting up with individuals from other states. When asked, "So who who who the dudes you supposed to been going you said tomorrow from where? Down south or from Virginia?" NORMAN replied, "Na from New Jersey." The male speaker then asked:

[MALE SPEAKER]: You by you by yourself?

NORMAN: Yeah, I'm by myself. Shine and all them are at the house.

[MALE SPEAKER]: Oh, okay. How much they going for?

NORMAN: For the part, thirty-five hundred. [unintelligible] About thirty-five hundred? I don't know if they gonna gamble on a little bit of what.

At approximately 6:27 a.m. on July 29, 2017, NORMAN described the scene of what is believed to be a dog fight, in a phone call with an unidentified male:

UNIDENTIFIED MALE: hey made it in?

NORMAN: yea yea, we just pulled up

UNIDENTIFIED MALE: ok, alot of people there?

NORMAN: no no no we're small - about 12 people

NORMAN and the same unidentified male spoke again at 7:22 a.m.:

UNIDENTIFIED MALE: it start yet?

NORMAN: yeah, we 15 minutes in

At approximately 9:36 a.m. that day, apparently after the dog fight ended, NORMAN provided a recap of a fight between Pyrex and another dog, where NORMAN described the other dog as follows:

NORMAN: Man, that dog wasn't shit man. First of all, that dog should've been a 32 anyway, first of all. The dog ain't have no ribs showing, had a gut. The dog came in injured, he already had a - he- he was bleeding, already had a cut on his leg....I'm like

UNIDENTIFIED MALE: Damn

NORMAN: What the fuck is going on man?

UNIDENTIFIED MALE: Damn.

NORMAN: I'm like...these dogs boy...

UNIDENTIFIED MALE: A cut on his leg?

NORMAN: Yeah, he brought him in the box bleeding...I'm like, this shit crazy.

UNIDENTIFIED MALE: And he was really a 32?

NORMAN: (yawning) yeah...(exhales) I was like man.....man oh man.

UNIDENTIFIED MALE: This shit is easy money though, I ain't gonna lie. It's easy money. It's no contest. It really isn't.

Later in this same phone call, NORMAN described more details of what appears to be the dog fight in which NORMAN's dog Pyrex participated:

NORMAN: I could see- but I could see it though. Cause he, he only was able to bite Pyrex like 4 or 5 times and when he bit him , I mean Pyrex had some crazy shit coming from his neck and his chest. Like, that shit like a turkey neck. Like that shit

(Talking over each other)

UNIDENTIFIED MALE: Oh so he had mouth?

NORMAN: Yeah, he had mouth. Hell yeah, he couldn't- he couldn't keep his mouth closed. [unintelligible] All kinds of shit.

UNIDENTIFIED MALE: The shaking was bad?

NORMAN: yea he did ride the head a little bit but that's not his style. If a dog troops a better face dog, I think they'll beat him. you know what i'm saying? I think they'll beat him, it's the truth

Later on in this same phone call, NORMAN appeared to begin to describe another dog of his who was expecting puppies:

NORMAN: yea that bitch is fly off the corners, fly off the corner. I ain't got too much fucking with her. out of two dogs, three dogs I would have put her through some shit she should have never been through man

UM: damn. you trying her quit man

RN: yea I tried to quit her cuz she um. grown up she did alot of dumb shit; fuck my yard up. I had her in the house one time, she got up and destroyed my house; just alot of personal shit i had with the dog. I wanted the bitch gone. and then when I finally got a match a couple times, she was just knocking handles out left and right. That dog, she crazy man. When she get amped up, she get crazy man she get amped up, she get really crazy. but that other one is the key bro. I can't wait for them to get together next time to get that going

f. The same day as the dog fight described above, later that morning, NORMAN had a phone conversation with his girlfriend. In that call, NORMAN described the

opposing dog in the dog fight as “a piece of shit dog,” and that “Pyrex ran right through him.” NORMAN further said of the opposing dog, “The dog came, man he was already bleeding, he had a big ass gash on his leg. He was- . . . bleeding when they brought him in the box.” NORMAN elaborated of the other dog in the fight, “Blood was leaking down his leg when they brought him in the box. . . . He had a gash on his leg. He had a gash on his leg, he was fat, and he came in overweight.” In criticizing that dog’s owner, NORMAN said, “Some niggas don’t be caring, some niggas will like try to put weight on they dog [unintelligible] ..and I know this what i do: but the last two weeks of this heat you’ll always see me weighing these dogs and weighing the food, it’s super important. But people get lazy with that, you know what I’m saying?”

g. Permission is sought to allow the FBI to obtain the assistance of Federal, State or local law enforcement authorities and the American Society for the Prevention of Cruelty to Animals (ASPCA) in executing the searches of the TARGET PREMISES and TARGET VEHICLES described in Attachment A-1 through A-4, respectively. Permission is also sought to allow these parties to seize items identified in Attachment B-1 through B-4 as well as to take photographs or video of any location, item, or individual at the search site, use water and electrical power at search site, to set up necessary equipment, and to establish safety perimeters as government agents deem necessary to accomplish the search. The government also seeks permission to allow animal technicians to enter the property to assist with handling of animals once the premises are secure and the search has been completed.

**D. TARGET PREMISES**

24. The TARGET PREMISES includes the residence located at 2442 Saint Clair Drive, Temple Hills, Maryland, and its curtilage, which is within the District of Maryland and is



described more particularly in Attachment A-1. Law enforcement surveillance has shown that the TARGET PREMISES are NORMAN's primary residence.

25. The investigation has also shown that NORMAN has appeared to be at the TARGET PREMISES while communicating with co-conspirators about some of the Fraud Scheme offenses. For example:

b. As described in more detail in the Criminal Complaint Affidavit, intercepted wire communications revealed that on July 3, 2017, NORMAN, who was using cellular telephone number (202) 600-0192, and WILLIAMS appeared to discuss encoding cards with a credit card writer. Cell-site location information for NORMAN's cellular telephone, obtained through a court order issued in the Eastern District of Virginia, revealed that at or around the time of this call, NORMAN was located in the vicinity of the TARGET PREMISES.

c. As described in more detail in the Criminal Complaint Affidavit, intercepted wire communications revealed that on July 9, 2017, at approximately 11:53 a.m., NORMAN and WILLIAMS discussed over the phone their purchases from a website that they appeared to be simultaneously accessing from a shared account. Cell-site location information from NORMAN's cellular telephone, obtained through a court order issued in the Eastern District of Virginia, revealed that at approximately 11:48 a.m. on July 9, 2017, NORMAN's cellular telephone was located in the vicinity of the TARGET PREMISES.

26. Additionally, investigation has shown that it appears co-conspirators in the Fraud Scheme offenses have visited NORMAN at the TARGET PREMISES. For example, on August 2, 2017, FBI physical surveillance observed co-conspirator RYAN MCNEIL, as described in more detail in the Criminal Complaint Affidavit, drive away from the TARGET PREMISES at approximately 2:43 p.m. Surveillance camera footage from that day showed that around or

shortly after 3:39 p.m., MCNEIL attempted to purchase cartons of cigarettes with fraudulent credit cards at a Sunoco gas station in Sterling, Virginia. After being confronted by a store manager, MCNEIL ran out of the store and drove off in his vehicle — the same vehicle earlier seen at the TARGET PREMISES. Four days later, in an intercepted wire communication on WILLIAMS's cellphone between WILLIAMS and NORMAN, NORMAN stated about MCNEIL, "He can't really focus to do good work, he sit in the car tryin to find girls, I just be givin him like 15 unless I leave out of town and he in a situation like he is now that he need bread then I'll give him like thirty-three-dollar pieces shit like that and see what he can get."

27. Investigation has shown that NORMAN has or does keep dogs at the TARGET PREMISES. On May 23, 2017, FBI physical surveillance observed NORMAN depart the TARGET PREMISES on a bicycle while leading a dog on a leash. FBI physical surveillance subsequently observed NORMAN and the dog arrive at NORMAN's known D.C. location which is approximately four miles away.

28. Intercepted phone conversations on NORMAN's cellphone, authorized by court order as described above, have also indicated that NORMAN keeps dogs and dog-fighting paraphernalia at the TARGET PREMISES. For example:

a. NORMAN has indicated in phone calls that he has special trainings and workouts for his dogs at his "house." In a phone call on August 2, 2017, with an unidentified male, NORMAN described working out his dogs during the "keep," a conditioning process described above that is characteristic of training dogs for dog fighting ventures. In this call, NORMAN referred to a dog named "Bruiser" and stated, "I got Bruiser on the mill early this morning like I do early in the morning I let him go on the emill cuz I got it at my house. I just let him walk up hill for an hour. But I don't count that as a workout, so what I do right now we just

you know its the first week of [unintelligible] just going 10 min on the [unintelligible]. Walk him a little bit. One thing about Luce and everybody the first two weeks of the keep is fun you know. You ain't exerting no energy."

b. In a July 30, 2017 phone call, NORMAN told an UNIDENTIFIED MALE, "I got 8 dogs in my yards. They stayed in my house the night before." Based on my knowledge of this investigation and the context of this conversation, I understand NORMAN's "yard" to refer to NORMAN's known D.C. location, and his house to refer to the TARGET PREMISES.

**E. TARGET VEHICLES 1-3**

29. During the course of its investigation, the FBI has seen NORMAN use all three of the TARGET VEHICLES (as further described in Attachments A-2, A-3, and A-4), which are all routinely parked at the TARGET PREMISES.

30. Intercepted wire communications from NORMAN's cellphone have revealed NORMAN using vehicles in furtherance of the conspiracy. On July 29, 2017, prior to the dogfight that day which NORMAN attended and where he exhibited Pyrex, NORMAN spoke with an unidentified individual about the location of the dogfight and where people were meeting. During the call, NORMAN told the individual, "Naw, wait. I gotta, I gotta both parties with, I got both dogs with me." NORMAN further stated, "I'm heading up 210. So they ain't gonna start on time cause its gonna start at 7." Based on my knowledge of the investigation, NORMAN's observed use of each TARGET VEHICLE, and NORMAN's observed method of transporting dogs, I believe that NORMAN likely used one of the TARGET VEHICLES to transport Pyrex to the dogfight.

31. FBI physical surveillance has observed TARGET VEHICLE 1 parked at the

CAN



TARGET PREMISES on multiple occasions, including April 24, 2017 and May 1, 2017. A search of Virginia DMV databases revealed that this vehicle is registered to NORMAN at a previous address associated with NORMAN in Ruther Glen, Virginia.

32. On April 25, 2017, FBI surveillance observed NORMAN and his girlfriend getting into TARGET VEHICLE 1 in the vicinity of the TARGET PREMISES. NORMAN's girlfriend got in the driver's seat while NORMAN went to the rear of the vehicle, put an animal crate in the rear compartment, and placed a brown pitbull-style dog inside the carrier. TARGET VEHICLE 1 then departed the TARGET PREMISES. Based on this information and my knowledge of the investigation, I believe that NORMAN may have used TARGET VEHICLE 1 in furtherance of the dogfighting conspiracy.

33. FBI surveillance has also observed NORMAN drive the TARGET VEHICLE 1. For instance, on June 2, 2017, FBI physical surveillance observed NORMAN drive TARGET VEHICLE 1 from the TARGET PREMISES to a Giant grocery store located in District Heights, Maryland. On July 1, 2017, in an intercepted wire communication on WILLIAMS's cellphone, NORMAN and WILLIAMS discussed how Giant was now accepting credit cards as payment for gift cards:

NORMAN: guess what Giant did

WILLIAMS: What

NORMAN: "We are glad to let you know that we are now accepting credit for all Visa/Mastercard gift cards."

WILLIAMS: oh again?

NORMAN: (laughs)

WILLIAMS: you said they are or they not?



NORMAN: They ARE, there's a big ass sign at every cash register saying we are glad to let you guys know that we now accepting credit for purchase of Visas/Mastercard and American express gift cards

WILLIAMS: Damn that sound kinda crazy though. might be some i don't know gotta try it though, gotta probably be Mastercard for sure

NORMAN: thats fine,

NORMAN: (Laughs) that won't be a problem

WILLIAMS: (Laughs)

34. FBI physical surveillance has observed TARGET VEHICLE 2 parked at the TARGET PREMISES on multiple occasions, including April 24, 2017, May 1, 2017, and August 1, 2017. A search of Virginia DMV databases revealed that this vehicle is registered to NORMAN's girlfriend, who also resides at the TARGET PREMISES, at an address in Norfolk, Virginia. On August 2, 2017, FBI physical surveillance observed NORMAN driving TARGET VEHICLE 2 as he departed from the TARGET PREMISES.

35. In phone calls intercepted, through court order, on WILLIAMS's cellphone, it appears that NORMAN has discussed leaving fraudulent, conspiracy-created credit cards in VEHICLE 2 for co-conspirators to retrieve. On July 22, 2017, in a 3:30 p.m. phone call between WILLIAMS and NORMAN, NORMAN stated that he would leave "joints" in his "Benz" for co-conspirator DENAE HORTON:

WILLIAMS: We did enough joints though

NORMAN: huh

WILLIAMS: We did enough joints

NORMAN: Yeah, she got 18 with the name on it, and i guess its like another three that its just whatever. So, yeah there is definitely enough

WILLIAMS: Oh Okay, so there is enough, alright, alright cool, alright good looking

NORMAN: Alright so look, um, they in my my car door, so just tell her when she pull up she can just go to the car, my um, of the Benz out front and just get them out the side door

WILLIAMS: The driver

NORMAN: Yeah driver door.

WILLIAMS: alright

As described in the Criminal Complaint Affidavit, in the context of this conversation and based on my knowledge of this investigation, I understand "joints" to refer to conspiracy-created credit cards or other access devices.

36. Approximately fifteen minutes later, in an intercepted call between HORTON and WILLIAMS, WILLIAMS relayed NORMAN's instructions about the "black Benz" (the same color and make of VEHICLE 2):

HORTON: Hey, I'm out here

WILLIAMS: All right look, he said he put them in his car, um you see like a black Benz parked out there, on that street

HORTON: It might be parked out front of here. Yeah I see it

WILLIAMS: Alright, he said its in the passenger door, I mean the driver's door, the driver's door.

HORTON: The driver's door. Alright. I have them

WILLIAMS: Alright man, good luck

Based on these conversations and my knowledge of the investigation, I believe that NORMAN may store fraudulent credit cards in his vehicle, or leave fraudulent credit cards in his vehicles to transfer those cards to co-conspirators covertly.

37. FBI physical surveillance has observed TARGET VEHICLE 3 parked at the TARGET PREMISES on multiple occasions. On May 1, 2017, physical surveillance observed TARGET VEHICLE 3 parked at the TARGET PREMISES. On this date, TARGET VEHICLE 3 bore Virginia registration VNP1059. An FBI review of Virginia DMV databases revealed that this registration corresponded to NORMAN at an address previously associated with him in Ruther Glen, Virginia. On July 24, 2017, FBI physical surveillance observed NORMAN depart the TARGET PREMISES carrying bags, which he then placed in TARGET VEHICLE 3. At that time, TARGET VEHICLE 3 bore Virginia registration VXR5749. FBI physical surveillance observed NORMAN then drive TARGET VEHICLE 3 to NORMAN's known second location in D.C., where NORMAN then carried the bags inside. An FBI review of Virginia DMV databases revealed that TARGET VEHICLE 3's new registration number (VXR5749) corresponded to Versa Traffic Management Group LLC, at the D.C. address where FBI believes NORMAN sometimes keeps his dogs.

#### **OTHER INFORMATION SUPPORTING PROBABLE CAUSE**

38. For the reasons stated in this affidavit, this search warrant application seeks authority to search the TARGET PREMISES, TARGET VEHICLES 1-3, and NORMAN for evidence relating to the TARGET OFFENSES in whatever form and whatever means they may have been created or stored, including any form of computer or electronic storage.

39. Investigation has shown that since at least 2015, NORMAN has participated in a fraud scheme to obtain stolen access device numbers, encode them onto credit cards and gift cards, and then use those access device cards to obtain, among other things, cartons of cigarettes for unlawful bulk resale. Investigation has shown that much of this conspiracy has been executed electronically — namely, through communications over electronic devices (including

devices belonging to NORMAN); access of websites that are believed to be black-market Internet sites that sell stolen credit card numbers; and the use of fraudulent and counterfeit access device cards that, when used in a transaction, cause the transmission of signals to confirm the validity of the card number. For example:

a. A September 2015 search warrant issued by Prince William County Circuit Court in Prince William County, Virginia, authorized the search of electronic devices belonging to WILLIAMS. These searches uncovered copies of text messages that were exchanged in March 2015 between WILLIAMS and NORMAN, who was saved into WILLIAMS's contact list by the nickname "Roddoe." These messages revealed that WILLIAMS and NORMAN communicated on or about March 28 and 29, 2015, about having credit cards forged in the name "Jefferey Scott." Additional text messages that were found showed that on July 2, 2017, NORMAN exchanged text messages with WILLIAMS and other co-conspirators where NORMAN requested reimbursement for credit card numbers that he had obtained. Other text messages recovered from WILLIAMS's devices revealed that in March 2015, WILLIAMS and NORMAN communicated about obtaining credit card numbers from the Internet site known as "Rescator." Through my research I have learned that "Rescator" is a known black-market website that facilitates the sale and distribution of stolen credit card data.

b. An April 4, 2017 search warrant issued by the Fairfax County Circuit Court in Fairfax County, Virginia, authorized the search of co-conspirator RYAN MCNEIL's cellphone. This search uncovered copies of text messages where NORMAN appeared to urge MCNEIL to continue using conspiracy-created credit cards to buy cartons of cigarettes. In one such text on September 22, 2016, MCNEIL wrote to NORMAN about the cards he had: "Most of them r duds. U do the math, 15 cartons out of 20 cards. 4 left." NORMAN replied, "Wow that's

fucking terrible.” In a text message on November 9, 2016, MCNEIL wrote to NORMAN, “Damn, i just got the last of what they had which was Marlboro light box.” In other text messages, NORMAN indicated that he was taking the bulk cigarette cartons to a buyer in New York: on March 9, 2017, NORMAN texted to MCNEIL, “Told you that I driving up tonight to take all the cigs to New York.”

c. Intercepted communications on WILLIAMS’s cellphone on July 9, 2017, indicated that WILLIAMS and NORMAN were on the phone with each other while simultaneously accessing a website where they seemed to share an account. WILLIAMS’s stated, “Yo, damn son, I didn’t see you putting this shit in the cart, so when I fucking click buy, and your shits is in there. So um, listen, on this cart I just bought son, just those first 13 is mine.” NORMAN responded, “Alright, hold on man, let me see.” WILLIAMS replied, “I got all the same shit for us, except for one. You see it?” Based on my knowledge of this investigation and the context of this conversation, as well my training and experience, I believe “cart” referred to an online shopping cart.

40. Investigation has also shown that NORMAN has himself been in possession of fraudulent access device cards. On or about July 14, 2015, NORMAN was identified by the Fairfax County Police Department (“FCPD”) when he attempted to use suspected fraudulent credit cards to make cigarette purchases at a Giant Food supermarket in Falls Church, Virginia. The Giant store manager reported to FCPD that NORMAN used or attempted to use four different credit cards to purchase two cartons of Newport cigarettes. According to the manager, the first three credit cards that NORMAN provided were rejected, but the fourth card NORMAN produced to complete the purchase was accepted by the store’s credit card system. The last four digits imprinted on the front of this credit card did not match the last four digits printed on the

store's mechanically generated receipt for the purchase, however. Upon request, NORMAN provided a driver's license to a store employee to confirm that his identity matched the name on this credit card. When the store manager informed NORMAN that based on suspected fraudulent activity, the store would keep the credit card and driver's license NORMAN had provided, NORMAN did not say anything and walked out of the store. Among other things, during this incident FCPD officers seized items that NORMAN had left behind at the Giant store, including a Bank of America Visa credit card that was imprinted with an account number on the front of the card that did not match the last four digits that were displayed – namely, the number on the card's magnetic strip – when the card was run through a credit card transaction machine.

41. Investigation has also shown that NORMAN may have in his possession or control a credit-card device reader/writer. For example, intercepted communications revealed that on July 3, 2017, NORMAN and WILLIAMS discussed encoding with a card writer (emphasis added):

WILLIAMS: I've been buying those shits for the last 3 days that Norfolk shit it was 1000 pieces in there.

NORMAN: Really?

WILLIAMS: more than 1000 yeah i bought all them shits

NORMAN: you bought all of what?

WILLIAMS: all of those f\*ing 427's man. there's like 8 maybe like 7 more up there. you gotta go get em man

NORMAN: how they do though?

WILLIAMS: they lit

NORMAN: oh im about to go get some right now



WILLIAMS: Put track one on those shits though

NORMAN: it was different?

WILLIAMS: yeah man i just figured it out yesterday you gotta put that Travon on there

NORMAN: from what store?

WILLIAMS: everywhere. just put it up there from now on bro. that's the new thing going on i think man

NORMAN: yeah, what's going on with **my joint** though. it won't let me do tracking that shit won't let me write that shit up.

WILLIAMS: oh, your shit f\*ing up? you probably need a new one.

NORMAN: when i put track one in there that shit says error.

WILLIAMS: oh, make sure you hit backspace when you do it cause you might have to backspace it. if it's like you know how the space gotta be right close to it, make sure you backspace it and then hit it then try it. Make sure you like once you once you once you copy and paste it hit backspace and make sure there's it it the cursor's right on the last number.

NORMAN: ok

WILLIAMS: and then it should work. cause it ain't gonna let you write it up if it's a space

Based on my knowledge of this case and the context of this conversation, as well as my training and experience, I believe NORMAN's reference to "my joint" that won't let him "do tracking" nor "write that shit up," refers to a card writer. The references to "Track 1" in the above excerpt are believed to refer to a particular track of data that is encoded to a credit card's magnetic stripe.

42. Based on my knowledge, training, and experience, as well as that of other agents in this investigation, I know that it is common for those involved in the manufacture, sale, purchase, and transportation of fraudulent credit cards (also known as access devices) and the merchandise purchased with such cards to generate and maintain writings, books, receipts,

business ledgers, lists, notations, money order transfers, or other memoranda and/or papers to assist in their criminal activity. These materials are created and maintained in much the same way and for the reasons as persons involved in legitimate business keep similar materials. Persons involved in the sale and purchase of fraudulent cards/devices will frequently keep materials memorializing past transactions, the status of accounts, inventories, income, and expense records, and the like, all of which are pieces of relevant evidence. Moreover, persons who create fraudulent cards/devices oftentimes use their residences to manufacture, package, distribute or transfer these items. I have learned it is common for those involved to secrete credit cards, proceeds, and records (including electronic records) of transactions and telephone numbers of their associates in the criminal enterprise in secure locations within their residences (including, but not limited to, attic, basement, crawl space, or other such areas therein), or the residences of their associates, to including the curtilages as well as vehicles or other structures located on the curtilage of such property, for ready access and to conceal the same from law enforcement.

43. Based on my knowledge, training, and experience, I have also learned that persons involved in access device fraud commonly maintain address or telephone numbers in books, papers, or electronic files which reflect names, addresses, and telephone numbers for their associates involved in the criminal conspiracy; that these conspirators frequently take or cause to be taken photographs of themselves, their associates, their property, or their proceeds, and frequently maintain these photographs in their possession and in their residences; that sometimes those involved in access device fraud use computers and electronic storage devices to list associates and keep track of debts, product on hand, proceeds, names, addresses, and telephone numbers of their associates. I have also learned that those involved in fraudulent credit card

schemes rely on timely telephonic communications to coordinate deals, such that they use telephones, often cellular telephones, to communicate amongst associates and co-conspirators in conducting transactions; that when using cellular telephones, sometimes they leave voice mail or text messages regarding their illegal activities; that cellular telephones often contain "telephone books" which reflect names, addresses, and/or telephone numbers of their associates in the criminal scheme; that cellular telephones also often keep track of recent outgoing and incoming telephone numbers; and that the cellular telephones used by conspirators are sometimes subscribed to in fictitious and/or other individuals' names.

44. Based on my knowledge, training, and experience, I have also learned that individuals using fraudulent credit cards frequently transport those cards, proceeds and devices in their vehicles when traveling to and from the location of a transaction. They may also store other property relating to their fraudulent credit card business in their vehicles, including cellular phones, writings, books, receipts, business ledgers, lists, notations, airline tickets, money order transfers, and other memoranda and/or papers relating to their criminal activities in their vehicles.

**COMPUTERS, TABLETS, WIRELESS TELEPHONES, AND OTHER ELECTRONIC DEVICES AND STORAGE MEDIA**

45. As described above and in Attachment B, these search warrants seek permission to search for records that might be found at the TARGET PREMISES, in TARGET VEHICLES 1-3, or on NORMAN's person or within his control, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, tablet, or other electronic devices or storage media (including scanners and printers with memory capability). Another form in which the records might be found is data stored on a wireless telephone. Thus, the warrants applied for would authorize the seizure of computers, tablets, wireless telephones,

and other electronic devices or storage media, and the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. If computers, tablets, wireless telephones, or other electronic devices or storage media are found at the TARGET PREMISES, in the TARGET VEHICLES, or on NORMAN's person or within his control, there is probable cause to believe records covered by these warrants will be stored on those devices, for at least the following reasons:

A. Based on my knowledge, training, and experience, I know that wireless telephones have capabilities that allow them to serve as: telephones, digital cameras, portable media players, GPS navigation devices, and personal digital assistants. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

B. Further, based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

C. In addition, based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto an electronic device, deleted, or viewed via the Internet. Electronic files downloaded to a computer, tablet, wireless telephone, or other electronic devices or storage media can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the electronic device until it is overwritten by new data.

D. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, for example, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

E. Wholly apart from user-generated files, electronic storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

F. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

47. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers, tablets, wireless telephones, or other electronic devices or storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer, tablets, wireless telephones, or other electronic devices or storage media at the TARGET PREMISES, in the TARGET VEHICLES, or on NORMAN’s person or within his control because:

A. Data on computers, tablets, wireless telephones, or other electronic devices or storage media can provide evidence of a file that was once on the computer, tablets, wireless telephones, or other electronic devices or storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the computer or other electronic devices or storage media that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times a computer was in use. Electronic device file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

B. As explained herein, information stored within a computer, tablets, wireless telephones, and other electronic devices or storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of a crime, or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or other electronic devices or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer, tablet, wireless telephone, or other electronic devices or storage media. This “user attribution” evidence is analogous to the search for “indicia



of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer, tablet, wireless telephone, or other electronic devices or storage media was remotely accessed, thus inculcating or exculpating its owner. Further, computer, tablet, wireless telephone, and other electronic devices or storage media activity can indicate how and when the device was accessed or used. For example, as described herein, computers, tablets, wireless telephones, or other electronic devices or storage media typically contain capabilities that log a variety of information, such as user account session times and durations, activity associated with user accounts, electronic storage media that connected with the computer, tablet, or wireless telephone, and the IP addresses through which the computer, tablet, wireless telephone, or other device accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer, tablet, wireless telephone, or other electronic devices or storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer, tablet, wireless telephone, or other electronic devices or storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a device may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the user of the computer, tablet, wireless telephone, or other electronic devices or storage media. Lastly, information stored within a computer, tablet, wireless telephone, or other electronic



devices or storage media may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer, tablet, wireless telephone, or other electronic devices or storage media may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

C. A person with appropriate familiarity with how computers, tablets, wireless telephones, or other electronic devices or storage media work can, after examining this forensic evidence in its proper context, draw conclusions about how computers, tablets, wireless telephones, and other electronic devices or storage media were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a computer, tablet, wireless telephone, or other electronic devices or storage media that is necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer, tablet, wireless telephone, or other electronic devices or storage media is evidence may depend on other information stored on the device and the application of knowledge about how a particular device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

E. Further, in finding evidence of how a computer, tablet, wireless telephone, or other electronic devices or storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a computer,



tablet, wireless telephone, or other electronic devices or storage media. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

48. In most cases, a thorough search of a premises for information that might be stored on computers, tablets, wireless telephones, or other electronic devices or storage media often requires the seizure of the physical computer, tablet, wireless telephone, or other electronic devices or storage media and later off-site review consistent with the warrants. In lieu of removing computers, tablets, wireless telephones, or other electronic devices or storage media from the premises, it is sometimes possible to make an image copy of the computer, tablet, wireless telephone, or other electronic devices or storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer, tablet, wireless telephone, or other electronic devices' or storage media's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the computer, tablet, wireless telephone, or other electronic device or storage medium, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

A. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer, tablet, wireless telephone, or other electronic devices or storage media has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine computers, tablets, wireless telephones, and other electronic devices or storage media to obtain evidence.

Computers, tablets, wireless telephones, and other electronic devices or storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

B. *Technical requirements.* Electronic devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on site. However, taking the computers, tablets, wireless telephones, or other electronic devices or storage media off-site and reviewing them in a controlled environment will allow their examination with the proper tools and knowledge.

C. *Variety of forms of electronic devices.* As described above, records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

49. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying computers, tablets, wireless telephones, and other electronic devices or storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the computer, tablets, wireless telephones, or other electronic devices or storage media pursuant to the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire computer, tablet, wireless telephone, or other electronic devices or storage media, that might expose many parts of the computer hard drive, tablet, wireless

telephone, or other electronic devices or storage media to human inspection in order to determine whether it is evidence described by the warrant.

### **LOCKED DEVICES WITH TOUCH ID**

50. This search warrant application also seeks authority for law enforcement to press the fingers (including thumbs) of NORMAN to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found at the TARGET PREMISES, in the TARGET VEHICLES 1-3, or on NORMAN's person or within his control, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by these warrants.

51. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature of Apple products is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents.

52. Upon information and belief, in some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead.

These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

53. The passcode or password that would unlock any Apple device(s) found during the search of the TARGET PREMISES, the TARGET VEHICLES, or NORMAN's person is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the Apple device(s) found during these searches to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the searches authorized by these warrants. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the searches authorized by these warrants.

54. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found at the TARGET PREMISES, in the TARGET VEHICLES, or on NORMAN's person or within his control, as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

55. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of NORMAN to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found at the TARGET PREMISES, in the TARGET VEHICLES, or on NORMAN's person or within his control, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by these warrants.

Can

### CONCLUSION

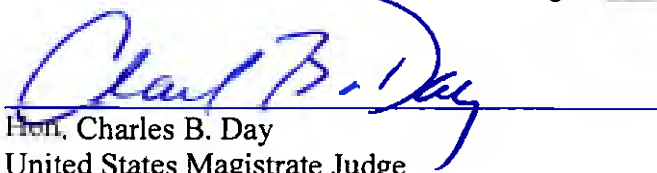
56. Based on the foregoing, I submit that probable cause exists that the evidence, fruits, or instrumentalities of the following criminal offenses are located at the TARGET PREMISES, in the TARGET VEHICLES 1-3, and on the person of NORMAN: 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1028 (identity theft), § 1029(a) (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud); § 2342 (trafficking of contraband cigarettes); §§ 1956 and 1957 (conspiracy to commit money laundering) (collectively, "Fraud Scheme offenses"); 21 U.S.C. §§ 841 and 846 (conspiracy to distribute oxycodone); and 7 U.S.C. § 2156 (unlawful animal fighting venture).

Respectfully submitted,



Charles B. Doughty  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on August 23, 2017



Hon. Charles B. Day  
United States Magistrate Judge

**ATTACHMENT A-1**

**Property to Be Searched**

The **TARGET PREMISES** include the residence located at 2442 St. Clair Drive, Temple Hills, MD, in the District of Maryland, as well as any vehicles, outbuildings, storage lockers (including safes) located thereon. The residence is further described as a detached single-family home, as depicted in the photograph below. The house is a light tan color with black shutters and has stairs that lead from the ground up to a landing at the white front door with oval-shaped glass inset into the door. The numbers 2442 are located to the left of the front door mounted to the brick side of the house.



CRA

**ATTACHMENT B-1**

1. Records, information, and items pertaining to the ownership, control, occupancy, residency, or maintenance of the SUBJECT PREMISES.
2. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy) and 7 U.S.C. § 2156 (unlawful animal fighting venture), including the following:
  - A. All live or dead dogs, including puppies born or unborn;
  - B. Other animals capable of being used in the dog fighting training process;
  - C. All dog fighting paraphernalia, including: treadmills for animals, exercise wheels, hides or other material used as hanging devices to strengthen or condition dogs; collars, leashes, chains, and other devices capable of being used to exercise or restrain fighting dogs; wooden sticks or handles capable of being used to pry open dogs' jaws; breeding stands; weight scales; and any washtubs, buckets, pails, and sponges capable of being used to wash dogs;
  - D. Animal-carrying cases, pens, chains, or leads;
  - E. Any constructed enclosures or components of any pits or enclosures capable of being used for the purpose of dog fighting, training dogs for fighting, or housing dogs intended to be used for fighting, including any carpeting or other materials used on the floor or walls of such enclosures;
  - F. Any writings, images, or videos that contain material that depicts or promotes dog fighting or training; including on electronically stored media;
  - G. Antibiotics, drugs, or vitamins capable of being used to treat injured dogs or to enhance their performance; needles and syringes capable of being used for the administration of such drugs; suture or surgical staple kits and other veterinary supplies; commercial dog food;



H. Any dog or other animal carcasses located or buried on the property, or parts or skins thereof;

I. Any flooring or wall components displaying evidence of blood, fur, or other animal matter;

J. Any utensils or weapons reasonably capable of being utilized in the killing of animals, to include ropes, wire, guns, rifles, spent shotgun shells, spent bullet cartridges;

K. Devices capable of being used to deter barking in dogs, including collars, sprays, and sonic emitters;

L. Registration papers or other materials (written or otherwise) showing ownership or transfer of dogs, including bills of sale, pedigrees, breeding records, transport documents, shipping records, certificates, receipts, and veterinary records; including on electronically stored media;

M. Any documents or records of financial accounts or transactions related to payment for or proceeds from or related to dogs, including account statements, deposits, withdrawals, checks, debits, wire transfers, or other documents; including on electronically stored media;

N. Any dog fighting records, including names and telephone numbers of persons suspected of being dog fighters; any rules, contracts, training logs, breeding records or other written agreements concerning the fighting of dogs; including on electronically stored media;

O. Any awards, trophies, plaques, or ribbons promoting or relating to dog fighting;

P. Any film, video or audio recordings of dog fighting activity, including on electronically stored media;

Q. Any and all records and documents intended for or indicating gambling activities including any cash or other things of value intended to be used for gambling purposes;

R. Material (e.g., from buccal (cheek) swabs) for DNA determination from all live dogs for purposes of comparison with other blood/tissue evidence;

S. Soil, blood, fur, animal skins and vegetation from the property to be used for forensic testing.

3. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841 and 846 (conspiracy to distribute oxycodone), including evidence relating to the prescribing, acquisition, order, purchase, packaging, possession, or distribution of oxycodone or other prescription pain medication;

4. All items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1028 (identity theft), § 1029(a) (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud); § 2342 (trafficking of contraband cigarettes); §§ 1956 and 1957 (conspiracy to commit money laundering), including the following:

A. Any physical equipment and supplies that can be used to manufacture, counterfeit, alter, or modify credit, debit, or gift cards, including any magnetic stripe code reading/encoding devices; card embossing devices; related software; and blank plastic card stock.

B. Any counterfeit access devices, unauthorized access devices, and false identification documents; and access device numbers including credit card and debit card numbers.

C. Cartons of cigarettes;

D. Records and information relating to the acquisition, order, purchase, packaging, creation, possession, encoding, distribution, manufacturing, or use of any access device numbers and access devices, including credit cards, debit cards, bank cards, and gift cards;

E. Records and information relating to the acquisition, order, purchase, packaging, possession, distribution, or use of fraudulent identities, including creation of fraudulent identification cards;

F. Records and information relating to the bulk transportation, possession, purchase, distribution, or sale of cigarettes;

G. Records and information relating to the identity or location of any of NORMAN's co-conspirators, including photographs;

H. Records, information, and items pertaining to the ownership, control, residency, occupancy, or use of the TARGET PREMISES, TARGET VEHICLE 1, TARGET VEHICLE 2, or TARGET VEHICLE 3;

I. Currency, financial instruments, or any other items of value or proceeds of the fraudulent scheme activities of NORMAN or his co-conspirators.

2. Computers, wireless telephones, or other electronic devices or storage media that may have been used as a means to commit the violations described above, including to communicate in furtherance of the violations.

3. For any computer, wireless telephone, or other electronic device or storage media whose seizure is otherwise authorized by this warrant, and any computer, wireless telephone, or other electronic device or storage media that contains or in which are stored records or information that is otherwise called for by this warrant:

A. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. Evidence of software that would allow others to control the computer, wireless telephone, or other electronic device or storage media, such as viruses, Trojan horses, and other forms of malicious software;

C. Evidence of security software designed to detect the types of malicious software described above;

D. Evidence of the lack of the types of malicious software described above, as well as evidence of the absence of security software designed to detect the types of malicious software described above;

E. Evidence indicating how and when the computer, wireless telephone, or other electronic device or storage media was accessed or used to determine the chronological context of device access and use and events relating to the crimes under investigation;

F. Evidence indicating the computer, wireless telephone, or other electronic device or storage media user's state of mind as it relates to the crimes under investigation;

G. Evidence of the attachment to a computer of a wireless telephone or other electronic devices or storage media, or similar containers for electronic evidence, or of a wireless telephone or storage medium to other computers or electronic devices;

H. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer, wireless telephone, or other electronic device or storage media;

I. Evidence of the times the computer, wireless telephone, or other electronic device or storage media was used;

J. Passwords, encryption keys, and other access devices that may be necessary to access the computer, wireless telephone, or other electronic device or storage media;

K. Documentation and manuals that may be necessary to access the computer, wireless telephone, or other electronic device or storage media or to conduct a forensic examination of the computer, wireless telephone, or other electronic device or storage media;

L. Records of or information about Internet Protocol addresses used by the computer, wireless telephone, or other electronic devices or storage media;

M. Records of, or information about, the computer's, wireless telephone's, or other electronic device's or storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

N. Contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers, wireless telephones, or other electronic devices or storage media to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, tablets, server computers, and network hardware.

The term “storage medium” or “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, other magnetic or optical media, and scanners and printers with memory capability.

During the execution of the search of the TARGET PREMISES described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of NORMAN to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found at the TARGET PREMISES, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

**ATTACHMENT A-2**

**Property to Be Searched**

**TARGET VEHICLE 1** is a gold 2004 BMW SUV that bears Virginia license plate number VVD4387 and vehicle identification number ("VIN") 5UXFA13514LU28537 ("TARGET VEHICLE 1).

CPA

**ATTACHMENT B-2**

1. Records, information, and items pertaining to the ownership, control, or maintenance of TARGET VEHICLE 1.

2. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy) and 7 U.S.C. § 2156 (unlawful animal fighting venture), including the following:

- A. All live or dead dogs, including puppies born or unborn;
- B. Other animals capable of being used in the dog fighting training process;
- C. All dog fighting paraphernalia, including: treadmills for animals, exercise wheels, hides or other material used as hanging devices to strengthen or condition dogs; collars, leashes, chains, and other devices capable of being used to exercise or restrain fighting dogs; wooden sticks or handles capable of being used to pry open dogs' jaws; breeding stands; weight scales; and any washtubs, buckets, pails, and sponges capable of being used to wash dogs;
- D. Animal-carrying cases, pens, chains, or leads;
- E. Any constructed enclosures or components of any pits or enclosures capable of being used for the purpose of dog fighting, training dogs for fighting, or housing dogs intended to be used for fighting, including any carpeting or other materials used on the floor or walls of such enclosures;
- F. Any writings, images, or videos that contain material that depicts or promotes dog fighting or training; including on electronically stored media;
- G. Antibiotics, drugs, or vitamins capable of being used to treat injured dogs or to enhance their performance; needles and syringes capable of being used for the administration of such drugs; suture or surgical staple kits and other veterinary supplies; commercial dog food;





H. Any dog or other animal carcasses located or buried on the property, or parts or skins thereof;

I. Any flooring or wall components displaying evidence of blood, fur, or other animal matter;

J. Any utensils or weapons reasonably capable of being utilized in the killing of animals, to include ropes, wire, guns, rifles, spent shotgun shells, spent bullet cartridges;

K. Devices capable of being used to deter barking in dogs, including collars, sprays, and sonic emitters;

L. Registration papers or other materials (written or otherwise) showing ownership or transfer of dogs, including bills of sale, pedigrees, breeding records, transport documents, shipping records, certificates, receipts, and veterinary records; including on electronically stored media;

M Any documents or records of financial accounts or transactions related to payment for or proceeds from or related to dogs, including account statements, deposits, withdrawals, checks, debits, wire transfers, or other documents; including on electronically stored media;

N. Any dog fighting records, including names and telephone numbers of persons suspected of being dog fighters; any rules, contracts, training logs, breeding records or other written agreements concerning the fighting of dogs; including on electronically stored media;

O. Any awards, trophies, plaques, or ribbons promoting or relating to dog fighting;

P. Any film, video or audio recordings of dog fighting activity, including on electronically stored media;

Q. Any and all records and documents intended for or indicating gambling activities including any cash or other things of value intended to be used for gambling purposes;

R. Material (e.g., from buccal (cheek) swabs) for DNA determination from all live dogs for purposes of comparison with other blood/tissue evidence;

S. Soil, blood, fur, animal skins and vegetation from the property to be used for forensic testing.

3. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841 and 846 (conspiracy to distribute oxycodone), including evidence relating to the prescribing, acquisition, order, purchase, packaging, possession, or distribution of oxycodone or other prescription pain medication;

4. All items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1028 (identity theft), § 1029(a) (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud); § 2342 (trafficking of contraband cigarettes); §§ 1956 and 1957 (conspiracy to commit money laundering), including the following:

A. Any physical equipment and supplies that can be used to manufacture, counterfeit, alter, or modify credit, debit, or gift cards, including any magnetic stripe code reading/encoding devices; card embossing devices; related software; and blank plastic card stock.

B. Any counterfeit access devices, unauthorized access devices, and false identification documents; and access device numbers including credit card and debit card numbers.

C. Cartons of cigarettes;

D. Records and information relating to the acquisition, order, purchase, packaging, creation, possession, encoding, distribution, manufacturing, or use of any access device numbers and access devices, including credit cards, debit cards, bank cards, and gift cards;

E. Records and information relating to the acquisition, order, purchase, packaging, possession, distribution, or use of fraudulent identities, including creation of fraudulent identification cards;

F. Records and information relating to the bulk transportation, possession, purchase, distribution, or sale of cigarettes;

G. Records and information relating to the identity or location of any of NORMAN's co-conspirators, including photographs;

H. Records, information, and items pertaining to the ownership, control, residency, occupancy, or use of the TARGET PREMISES, TARGET VEHICLE 1, TARGET VEHICLE 2, or TARGET VEHICLE 3;

I. Currency, financial instruments, or any other items of value or proceeds of the fraudulent scheme activities of NORMAN or his co-conspirators.

5. Computers, wireless telephones, or other electronic devices or storage media that may have been used as a means to commit the violations described above, including to communicate in furtherance of the violations.

6. For any computer, wireless telephone, or other electronic device or storage media whose seizure is otherwise authorized by this warrant, and any computer, wireless telephone, or other electronic device or storage media that contains or in which are stored records or information that is otherwise called for by this warrant:

A. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. Evidence of software that would allow others to control the computer, wireless telephone, or other electronic device or storage media, such as viruses, Trojan horses, and other forms of malicious software;

C. Evidence of security software designed to detect the types of malicious software described above;

D. Evidence of the lack of the types of malicious software described above, as well as evidence of the absence of security software designed to detect the types of malicious software described above;

E. Evidence indicating how and when the computer, wireless telephone, or other electronic device or storage media was accessed or used to determine the chronological context of device access and use and events relating to the crimes under investigation;

F. Evidence indicating the computer, wireless telephone, or other electronic device or storage media user's state of mind as it relates to the crimes under investigation;

G. Evidence of the attachment to a computer of a wireless telephone or other electronic devices or storage media, or similar containers for electronic evidence, or of a wireless telephone or storage medium to other computers or electronic devices;

H. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer, wireless telephone, or other electronic device or storage media;

I. Evidence of the times the computer, wireless telephone, or other electronic device or storage media was used;

J. Passwords, encryption keys, and other access devices that may be necessary to access the computer, wireless telephone, or other electronic device or storage media;

K. Documentation and manuals that may be necessary to access the computer, wireless telephone, or other electronic device or storage media or to conduct a forensic examination of the computer, wireless telephone, or other electronic device or storage media;

L. Records of or information about Internet Protocol addresses used by the computer, wireless telephone, or other electronic devices or storage media;

M. Records of, or information about, the computer's, wireless telephone's, or other electronic device's or storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

N. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, tablets, server computers, and network hardware.

The term "storage medium" or "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, other magnetic or optical media, and scanners and printers with memory capability.

During the execution of the search of TARGET VEHICLE 1 described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of NORMAN to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found in TARGET VEHICLE 1, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

**ATTACHMENT A-3**

**Property to Be Searched**

**TARGET VEHICLE 2** is a black 2006 Mercedes sedan that bears Virginia license plate number VXR5729 and VIN number WDDDJ75X96A057 (“TARGET VEHICLE 2”).

A handwritten signature in blue ink, located in the bottom right corner of the page. The signature appears to be 'CBA' with a stylized flourish above it.

**ATTACHMENT B-3**

1. Records, information, and items pertaining to the ownership, control, or maintenance of TARGET VEHICLE 2.

2. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy) and 7 U.S.C. § 2156 (unlawful animal fighting venture), including the following:

- A. All live or dead dogs, including puppies born or unborn;
- B. Other animals capable of being used in the dog fighting training process;
- C. All dog fighting paraphernalia, including: treadmills for animals, exercise wheels, hides or other material used as hanging devices to strengthen or condition dogs; collars, leashes, chains, and other devices capable of being used to exercise or restrain fighting dogs; wooden sticks or handles capable of being used to pry open dogs' jaws; breeding stands; weight scales; and any washtubs, buckets, pails, and sponges capable of being used to wash dogs;
- D. Animal-carrying cases, pens, chains, or leads;
- E. Any constructed enclosures or components of any pits or enclosures capable of being used for the purpose of dog fighting, training dogs for fighting, or housing dogs intended to be used for fighting, including any carpeting or other materials used on the floor or walls of such enclosures;
- F. Any writings, images, or videos that contain material that depicts or promotes dog fighting or training; including on electronically stored media;
- G. Antibiotics, drugs, or vitamins capable of being used to treat injured dogs or to enhance their performance; needles and syringes capable of being used for the administration of such drugs; suture or surgical staple kits and other veterinary supplies; commercial dog food;



H. Any dog or other animal carcasses located or buried on the property, or parts or skins thereof;

I. Any flooring or wall components displaying evidence of blood, fur, or other animal matter;

J. Any utensils or weapons reasonably capable of being utilized in the killing of animals, to include ropes, wire, guns, rifles, spent shotgun shells, spent bullet cartridges;

K. Devices capable of being used to deter barking in dogs, including collars, sprays, and sonic emitters;

L. Registration papers or other materials (written or otherwise) showing ownership or transfer of dogs, including bills of sale, pedigrees, breeding records, transport documents, shipping records, certificates, receipts, and veterinary records; including on electronically stored media;

M. Any documents or records of financial accounts or transactions related to payment for or proceeds from or related to dogs, including account statements, deposits, withdrawals, checks, debits, wire transfers, or other documents; including on electronically stored media;

N. Any dog fighting records, including names and telephone numbers of persons suspected of being dog fighters; any rules, contracts, training logs, breeding records or other written agreements concerning the fighting of dogs; including on electronically stored media;

O. Any awards, trophies, plaques, or ribbons promoting or relating to dog fighting;

P. Any film, video or audio recordings of dog fighting activity, including on electronically stored media;

Q. Any and all records and documents intended for or indicating gambling activities including any cash or other things of value intended to be used for gambling purposes;

R. Material (e.g., from buccal (cheek) swabs) for DNA determination from all live dogs for purposes of comparison with other blood/tissue evidence;

S. Soil, blood, fur, animal skins and vegetation from the property to be used for forensic testing.

3. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841 and 846 (conspiracy to distribute oxycodone), including evidence relating to the prescribing, acquisition, order, purchase, packaging, possession, or distribution of oxycodone or other prescription pain medication;

4. All items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1028 (identity theft), § 1029(a) (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud); § 2342 (trafficking of contraband cigarettes); §§ 1956 and 1957 (conspiracy to commit money laundering), including the following:

A. Any physical equipment and supplies that can be used to manufacture, counterfeit, alter, or modify credit, debit, or gift cards, including any magnetic stripe code reading/encoding devices; card embossing devices; related software; and blank plastic card stock.

B. Any counterfeit access devices, unauthorized access devices, and false identification documents; and access device numbers including credit card and debit card numbers.

C. Cartons of cigarettes;

D. Records and information relating to the acquisition, order, purchase, packaging, creation, possession, encoding, distribution, manufacturing, or use of any access device numbers and access devices, including credit cards, debit cards, bank cards, and gift cards;

E. Records and information relating to the acquisition, order, purchase, packaging, possession, distribution, or use of fraudulent identities, including creation of fraudulent identification cards;

F. Records and information relating to the bulk transportation, possession, purchase, distribution, or sale of cigarettes;

G. Records and information relating to the identity or location of any of NORMAN's co-conspirators, including photographs;

H. Records, information, and items pertaining to the ownership, control, residency, occupancy, or use of the TARGET PREMISES, TARGET VEHICLE 1, TARGET VEHICLE 2, or TARGET VEHICLE 3;

I. Currency, financial instruments, or any other items of value or proceeds of the fraudulent scheme activities of NORMAN or his co-conspirators.

5. Computers, wireless telephones, or other electronic devices or storage media that may have been used as a means to commit the violations described above, including to communicate in furtherance of the violations.

6. For any computer, wireless telephone, or other electronic device or storage media whose seizure is otherwise authorized by this warrant, and any computer, wireless telephone, or other electronic device or storage media that contains or in which are stored records or information that is otherwise called for by this warrant:

A. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. Evidence of software that would allow others to control the computer, wireless telephone, or other electronic device or storage media, such as viruses, Trojan horses, and other forms of malicious software;

C. Evidence of security software designed to detect the types of malicious software described above;

D. Evidence of the lack of the types of malicious software described above, as well as evidence of the absence of security software designed to detect the types of malicious software described above;

E. Evidence indicating how and when the computer, wireless telephone, or other electronic device or storage media was accessed or used to determine the chronological context of device access and use and events relating to the crimes under investigation;

F. Evidence indicating the computer, wireless telephone, or other electronic device or storage media user's state of mind as it relates to the crimes under investigation;

G. Evidence of the attachment to a computer of a wireless telephone or other electronic devices or storage media, or similar containers for electronic evidence, or of a wireless telephone or storage medium to other computers or electronic devices;

H. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer, wireless telephone, or other electronic device or storage media;

I. Evidence of the times the computer, wireless telephone, or other electronic device or storage media was used;

J. Passwords, encryption keys, and other access devices that may be necessary to access the computer, wireless telephone, or other electronic device or storage media;

K. Documentation and manuals that may be necessary to access the computer, wireless telephone, or other electronic device or storage media or to conduct a forensic examination of the computer, wireless telephone, or other electronic device or storage media;

L. Records of or information about Internet Protocol addresses used by the computer, wireless telephone, or other electronic devices or storage media;

M. Records of, or information about, the computer's, wireless telephone's, or other electronic device's or storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

N. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, tablets, server computers, and network hardware.

The term "storage medium" or "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, other magnetic or optical media, and scanners and printers with memory capability.

During the execution of the search of TARGET VEHICLE 2 described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of NORMAN to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found in TARGET VEHICLE 2, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

**ATTACHMENT A-4**

**Property to Be Searched**

**TARGET VEHICLE 3** is white 1998 Ford truck that bears Virginia license plate number VXR5749 and VIN number 1FTZF1720WNB46350 ("TARGET VEHICLE 3").

CBD  
CBA

**ATTACHMENT B-4**

1. Records, information, and items pertaining to the ownership, control, or maintenance of TARGET VEHICLE 3.

2. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy) and 7 U.S.C. § 2156 (unlawful animal fighting venture), including the following:

- A. All live or dead dogs, including puppies born or unborn;
- B. Other animals capable of being used in the dog fighting training process;
- C. All dog fighting paraphernalia, including: treadmills for animals, exercise wheels, hides or other material used as hanging devices to strengthen or condition dogs; collars, leashes, chains, and other devices capable of being used to exercise or restrain fighting dogs; wooden sticks or handles capable of being used to pry open dogs' jaws; breeding stands; weight scales; and any washtubs, buckets, pails, and sponges capable of being used to wash dogs;
- D. Animal-carrying cases, pens, chains, or leads;
- E. Any constructed enclosures or components of any pits or enclosures capable of being used for the purpose of dog fighting, training dogs for fighting, or housing dogs intended to be used for fighting, including any carpeting or other materials used on the floor or walls of such enclosures;
- F. Any writings, images, or videos that contain material that depicts or promotes dog fighting or training; including on electronically stored media;
- G. Antibiotics, drugs, or vitamins capable of being used to treat injured dogs or to enhance their performance; needles and syringes capable of being used for the administration of such drugs; suture or surgical staple kits and other veterinary supplies; commercial dog food;



H. Any dog or other animal carcasses located or buried on the property, or parts or skins thereof;

I. Any flooring or wall components displaying evidence of blood, fur, or other animal matter;

J. Any utensils or weapons reasonably capable of being utilized in the killing of animals, to include ropes, wire, guns, rifles, spent shotgun shells, spent bullet cartridges;

K. Devices capable of being used to deter barking in dogs, including collars, sprays, and sonic emitters;

L. Registration papers or other materials (written or otherwise) showing ownership or transfer of dogs, including bills of sale, pedigrees, breeding records, transport documents, shipping records, certificates, receipts, and veterinary records; including on electronically stored media;

M. Any documents or records of financial accounts or transactions related to payment for or proceeds from or related to dogs, including account statements, deposits, withdrawals, checks, debits, wire transfers, or other documents; including on electronically stored media;

N. Any dog fighting records, including names and telephone numbers of persons suspected of being dog fighters; any rules, contracts, training logs, breeding records or other written agreements concerning the fighting of dogs; including on electronically stored media;

O. Any awards, trophies, plaques, or ribbons promoting or relating to dog fighting;

P. Any film, video or audio recordings of dog fighting activity, including on electronically stored media;

Q. Any and all records and documents intended for or indicating gambling activities including any cash or other things of value intended to be used for gambling purposes;

R. Material (e.g., from buccal (cheek) swabs) for DNA determination from all live dogs for purposes of comparison with other blood/tissue evidence;

S. Soil, blood, fur, animal skins and vegetation from the property to be used for forensic testing.

3. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841 and 846 (conspiracy to distribute oxycodone), including evidence relating to the prescribing, acquisition, order, purchase, packaging, possession, or distribution of oxycodone or other prescription pain medication;

4. All items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1028 (identity theft), § 1029(a) (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud); § 2342 (trafficking of contraband cigarettes); §§ 1956 and 1957 (conspiracy to commit money laundering), including the following:

A. Any physical equipment and supplies that can be used to manufacture, counterfeit, alter, or modify credit, debit, or gift cards, including any magnetic stripe code reading/encoding devices; card embossing devices; related software; and blank plastic card stock.

B. Any counterfeit access devices, unauthorized access devices, and false identification documents; and access device numbers including credit card and debit card numbers.

C. Cartons of cigarettes;

D. Records and information relating to the acquisition, order, purchase, packaging, creation, possession, encoding, distribution, manufacturing, or use of any access device numbers and access devices, including credit cards, debit cards, bank cards, and gift cards;

E. Records and information relating to the acquisition, order, purchase, packaging, possession, distribution, or use of fraudulent identities, including creation of fraudulent identification cards;

F. Records and information relating to the bulk transportation, possession, purchase, distribution, or sale of cigarettes;

G. Records and information relating to the identity or location of any of NORMAN's co-conspirators, including photographs;

H. Records, information, and items pertaining to the ownership, control, residency, occupancy, or use of the TARGET PREMISES, TARGET VEHICLE 1, TARGET VEHICLE 2, or TARGET VEHICLE 3;

I. Currency, financial instruments, or any other items of value or proceeds of the fraudulent scheme activities of NORMAN or his co-conspirators.

5. Computers, wireless telephones, or other electronic devices or storage media that may have been used as a means to commit the violations described above, including to communicate in furtherance of the violations.

6. For any computer, wireless telephone, or other electronic device or storage media whose seizure is otherwise authorized by this warrant, and any computer, wireless telephone, or other electronic device or storage media that contains or in which are stored records or information that is otherwise called for by this warrant:

A. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. Evidence of software that would allow others to control the computer, wireless telephone, or other electronic device or storage media, such as viruses, Trojan horses, and other forms of malicious software;

C. Evidence of security software designed to detect the types of malicious software described above;

D. Evidence of the lack of the types of malicious software described above, as well as evidence of the absence of security software designed to detect the types of malicious software described above;

E. Evidence indicating how and when the computer, wireless telephone, or other electronic device or storage media was accessed or used to determine the chronological context of device access and use and events relating to the crimes under investigation;

F. Evidence indicating the computer, wireless telephone, or other electronic device or storage media user's state of mind as it relates to the crimes under investigation;

G. Evidence of the attachment to a computer of a wireless telephone or other electronic devices or storage media, or similar containers for electronic evidence, or of a wireless telephone or storage medium to other computers or electronic devices;

H. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer, wireless telephone, or other electronic device or storage media;

I. Evidence of the times the computer, wireless telephone, or other electronic device or storage media was used;

J. Passwords, encryption keys, and other access devices that may be necessary to access the computer, wireless telephone, or other electronic device or storage media;

K. Documentation and manuals that may be necessary to access the computer, wireless telephone, or other electronic device or storage media or to conduct a forensic examination of the computer, wireless telephone, or other electronic device or storage media;

L. Records of or information about Internet Protocol addresses used by the computer, wireless telephone, or other electronic devices or storage media;

M. Records of, or information about, the computer's, wireless telephone's, or other electronic device's or storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

N. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, tablets, server computers, and network hardware.

The term "storage medium" or "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, other magnetic or optical media, and scanners and printers with memory capability.

During the execution of the search of TARGET VEHICLE 3 described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of NORMAN to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found in TARGET VEHICLE 3, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

**ATTACHMENT A-5**

**Person to Be Searched**

As depicted in the images below, **RODRIGUEZ RODNEY LOMAX NORMAN**, a/k/a “Roddoe,” is to be searched, as well as any electronic devices (e.g., computers, wireless telephones, and other electronic devices or storage media, such as scanners, external storage media, and printers with memory capability) located on his person or within his control. **NORMAN** is approximately 31 years old and is a black male with black hair and dark colored eyes.



CM  
CR

**ATTACHMENT B-5**

1. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy) and 7 U.S.C. § 2156 (unlawful animal fighting venture), including the following:

A. All dog fighting paraphernalia, including: collars, leashes, chains, and other devices capable of being used to exercise or restrain fighting dogs; wooden sticks or handles capable of being used to pry open dogs' jaws;

B. Animal-carrying cases, pens, chains, or leads;

C. Any writings, images, or videos that contain material that depicts or promotes dog fighting or training; including on electronically stored media;

D. Antibiotics, drugs, or vitamins capable of being used to treat injured dogs or to enhance their performance; needles and syringes capable of being used for the administration of such drugs; suture or surgical staple kits and other veterinary supplies; commercial dog food;

E. Any utensils or weapons reasonably capable of being utilized in the killing of animals, to include ropes, wire, guns, rifles, spent shotgun shells, spent bullet cartridges;

F. Devices capable of being used to deter barking in dogs, including collars, sprays, and sonic emitters;

G. Registration papers or other materials (written or otherwise) showing ownership or transfer of dogs, including bills of sale, pedigrees, breeding records, transport documents, shipping records, certificates, receipts, and veterinary records; including on electronically stored media;



H. Any documents or records of financial accounts or transactions related to payment for or proceeds from or related to dogs, including account statements, deposits, withdrawals, checks, debits, wire transfers, or other documents; including on electronically stored media;

I. Any dog fighting records, including names and telephone numbers of persons suspected of being dog fighters; any rules, contracts, training logs, breeding records or other written agreements concerning the fighting of dogs; including on electronically stored media;

J. Any film, video or audio recordings of dog fighting activity, including on electronically stored media;

K. Any and all records and documents intended for or indicating gambling activities including any cash or other things of value intended to be used for gambling purposes;

2. Records, information, and items that constitute fruits, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841 and 846 (conspiracy to distribute oxycodone), including evidence relating to the prescribing, acquisition, order, purchase, packaging, possession, or distribution of oxycodone or other prescription pain medication;

3. All items that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1028 (identity theft), § 1029(a) (access device fraud), § 1343 (wire fraud), § 1344 (bank fraud); § 2342 (trafficking of contraband cigarettes); §§ 1956 and 1957 (conspiracy to commit money laundering), including the following:

A. Any physical equipment and supplies that can be used to manufacture, counterfeit, alter, or modify credit, debit, or gift cards, including any magnetic stripe code reading/encoding devices; card embossing devices; related software; and blank plastic card stock.

B. Any counterfeit access devices, unauthorized access devices, and false identification documents; and access device numbers including credit card and debit card numbers.

C. Cartons of cigarettes;

D. Records and information relating to the acquisition, order, purchase, packaging, creation, possession, encoding, distribution, manufacturing, or use of any access device numbers and access devices, including credit cards, debit cards, bank cards, and gift cards;

E. Records and information relating to the acquisition, order, purchase, packaging, possession, distribution, or use of fraudulent identities, including creation of fraudulent identification cards;

F. Records and information relating to the bulk transportation, possession, purchase, distribution, or sale of cigarettes;

G. Records and information relating to the identity or location of any of NORMAN's co-conspirators, including photographs;

H. Records, information, and items pertaining to the ownership, control, residency, occupancy, or use of the TARGET PREMISES, TARGET VEHICLE 1, TARGET VEHICLE 2, or TARGET VEHICLE 3;

I. Currency, financial instruments, or any other items of value or proceeds of the fraudulent scheme activities of NORMAN or his co-conspirators.

4. Computers, wireless telephones, or other electronic devices or storage media that may have been used as a means to commit the violations described above, including to communicate in furtherance of the violations and/or generating or transmitting fraudulent invoices.

5. For any computer, wireless telephone, or other electronic device or storage media whose seizure is otherwise authorized by this warrant, and any computer, wireless telephone, or other electronic device or storage media that contains or in which are stored records or information that is otherwise called for by this warrant:

A. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. Evidence of software that would allow others to control the computer, wireless telephone, or other electronic device or storage media, such as viruses, Trojan horses, and other forms of malicious software;

C. Evidence of security software designed to detect the types of malicious software described above;

D. Evidence of the lack of the types of malicious software described above, as well as evidence of the absence of security software designed to detect the types of malicious software described above;

E. Evidence indicating how and when the computer, wireless telephone, or other electronic device or storage media was accessed or used to determine the chronological context of device access and use and events relating to the crimes under investigation;

F. Evidence indicating the computer, wireless telephone, or other electronic device or storage media user's state of mind as it relates to the crimes under investigation;

G. Evidence of the attachment to a computer of a wireless telephone or other electronic devices or storage media, or similar containers for electronic evidence, or of a wireless telephone or storage medium to other computers or electronic devices;

H. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer, wireless telephone, or other electronic device or storage media;

I. Evidence of the times the computer, wireless telephone, or other electronic device or storage media was used;

J. Passwords, encryption keys, and other access devices that may be necessary to access the computer, wireless telephone, or other electronic device or storage media;

K. Documentation and manuals that may be necessary to access the computer, wireless telephone, or other electronic device or storage media or to conduct a forensic examination of the computer, wireless telephone, or other electronic device or storage media;

L. Records of or information about Internet Protocol addresses used by the computer, wireless telephone, or other electronic devices or storage media;

M. Records of, or information about, the computer's, wireless telephone's, or other electronic device's or storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

N. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, tablets, server computers, and network hardware.

The term “storage medium” or “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, other magnetic or optical media, and scanners and printers with memory capability.

During the execution of the search of NORMAN’s person and the area within his control described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of NORMAN to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found on the person or within the control of NORMAN, for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

